

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Seizure and Search of:)

USA vs. 20-10-05)

Case No. 5:20-mj-213)
)
)
)
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed (*identify the person or describe the property to be seized*):

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2251

18 U.S.C. § 2422(b)

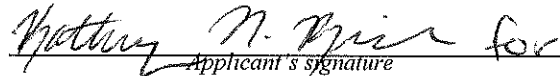
Offense Description

Attempted Sexual Exploitation of a Minor

Attempted Enticement of a Minor

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.


 Applicant's signature

Sarah B. Collins, AUSA

Printed name and title

Sworn to before me and: ☐ signed in my presence.

☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: 10/30/20


 Judge's signature

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate

Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

IN THE MATTER OF THE SEIZURE AND
SEARCH OF:

CASE NUMBER: 5:20-mj-213

USA vs. 20-10-05

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION**

REDACTED

State of South Dakota)
) ss
County of Pennington)

I, Brian Freeouf, Special Agent with the South Dakota Division of Criminal Investigation (DCI), being duly sworn, state as follows:

1. I began my law enforcement career with the Pennington County Sheriff's Office in July of 2005. I spent approximately three years on patrol in Wall, SD. In 2008, I joined the patrol division in Rapid City. I was promoted to the rank of Senior Deputy, in July of 2010. I also spent time as a School Liaison Officer and Criminal Investigations Division as a property crimes investigator. Even though I was assigned as a property crimes investigator, I also investigated other crimes but not limited to homicides, rapes, assaults, and coroner duties. My other assignments within the Sheriff's Office include Deputy Coroner, Field Training Deputy, and Defensive Tactics Training Administrator. Since November of 2014, I have been assigned to the ICAC Task Force (Internet Crimes against Children). The investigations worked by this unit include child pornography, solicitation of minors, sexual exploitation of minors, disseminating harmful materials to minors, and human trafficking. In January 2020, I became a Special

Agent with the South Dakota Division of Criminal Investigations. I remain assigned to the ICAC Task Force and continue investigations as listed above.

During my law enforcement career I have become familiar with the *modus operandi* of persons involved in attempted commercial sex trafficking of a minor, in violation of federal law. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally attempt to meet with children in order to engage in criminal sex acts.

2. The information set forth below is based upon my knowledge of an investigation conducted by the South Dakota Internet Crimes Against Children Taskforce (ICAC) and the investigation of other law enforcement agents and officers including, but not limited to, South Dakota Division of Criminal Investigation (DCI), Homeland Security Investigations (HSI), the Rapid City Police Department, and the Pennington County Sheriff's Office. I have not included every fact obtained pursuant to this investigation, but have set forth those facts that I believe are essential to establish the necessary probable cause for the criminal complaint. I have not omitted any material fact relevant to the consideration of probable cause for a criminal complaint against the above named defendant.

3. I have been informed that 18 U.S.C. § 2422(b) makes it a crime for a person to knowingly attempt to engage in enticement of a minor using the internet. I have also been informed that 18 U.S.C. § 2251 makes it a crime for a person to attempt to cause a minor to produce child pornography images.

1. Your affiant respectfully submits that there is probable cause to believe that Bernard Andrew Wagner, Jr. committed the crimes of attempted enticement of a minor using the internet and attempted sexual exploitation of a minor and utilized the SUBJECT DEVICES to commit the crime.

ITEMS TO BE SEARCHED FOR AND SEIZED:

2. The undersigned respectfully requests that a search warrant be issued to permit a search of the content of two cellular phones obtained during the search and arrest of Bernard Andrew Wagner, Jr. They are:

- One black Samsung Galaxy S9 in black case. IMEI: 353305092632468; and
- One black Motorola Tacfone. Model XT2005DL IMEI: 352180103523696

3. The warrant is sought in order to search for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b), enticement of a minor using the internet and 18 U.S.C. 18 U.S.C. § 2251, attempted sexual exploitation of a minor.

DEFINITIONS

4. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. *Child Erotica*: as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. *Child pornography*: as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. *Cloud-based storage service*: as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file.

Access is free and readily available to anyone who has an internet connection.

e. *Computer:* The term “computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.

f. *Computer Hardware:* The term “computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. *Computer-related documentation:* as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. *Computer Passwords and Data Security Devices:* The term “computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. *Computer-Related Documentation:* The term “computer-related documentation” means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. *Computer Software:* The term “computer software” means digital information which can be interpreted by a computer and any of its

related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. *Electronic Communication Service* (“ESP”): as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

l. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

m. *File Transfer Protocol* (“FTP”): as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. *Internet*: The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet

often cross state and international borders, even when the devices communicating with each other are in the same state.

o. *Internet Connection*: The term “Internet connection” means a connection required for access to the Internet. The connection would generally be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.

p. *Minor*: The term “minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

q. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. *Remote Computing Service* (“RCS”): as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. *Short Message Service* (“SMS”): as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage

facility or communications facility directly related to or operating in conjunction with such device.

t. *Storage Medium:* The term “storage medium” refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

u. *Visual Depictions:* “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

v. *Wireless Network:* The term “wireless network” means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer, which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any

resources available on that network to include other computers or shared Internet connections.

PROBABLE CAUSE

5. During the week of August 10, 2020, I received a report from the Spearfish Police Department of a minor possibly being solicited over text messages. This report indicated Bernard Wagner was sending inappropriate messages to a juvenile female "M.R." via text message. Bernard has known M.R. personally through various community events.

6. Bernard indicated to M.R. that he had a man problem and it was hard to deal with due to the fact he was so large. Bernard was conveying to M.R. that he had a large penis and scrotum. He sent her multiple images of himself wearing tight underwear and a tight swimsuit. The outline of Bernard's genitals is clearly visible, and photos were taken using a "selfie Stick", to where he focused the camera on his genitals. Bernard also indicated he needed "to get layed" and it was hard to sleep due to the size of his genitals.

7. Spearfish Police Department Detective Collin Smith generated a report, which I reviewed. It contains initial interviews with the victim MR and her mother Donna Reece. After reviewing the report, I contacted Donna Reece. She told him Bernard has still sent M.R. messages like "good morning" and "what are you doing today?". M.R. has not responded to him in any way. I advised Donna he would be contacting Bernard in an undercover capacity and stating he was one of M.R. friends and Donna agreed.

8. On September 14, 2020, I used a persona of a 15-year-old girl and started to text Bernard from an undercover phone number. The following is a brief overview of the information so far that has been exchanged between Bernard Wagner and me:

UC: "Hey im one of Maddys friends from Rapid I got your number from her"

After this message, the undercover received a phone call from 605-580-6975, which was listed as a Spearfish phone number. I did not answer this call and texted the original number.

UC: "did u just try to call? Cant talk im doing school stuff"

BW: "Yes text on that number please ty"

At this point I texted Bernard on the phone number 605-580-6975.

BW: "From Barney text this number"

BW: "what is your name"

UC: "Candice"

BW: "can you send me a picture of you"

UC: "I thought your name was Bernard not barney"

Bernard sent the UC a photo of himself not wearing a shirt. His face is visible in the image and it appears to be the same man the original victim MR was chatting with.

BW: "I goby Barney"

I sent him an image of his undercover persona. The image was age regressed and of a subject associated with law enforcement.

BW: "Very pretty do you like pictues"

UC: "Yeah I am taking a photography class in school"

BW: "What about naughty ones"

UC: "well depends since im 15 I could get in trouble" "But im down with whatever"

BW: "I'm very large I'm shure you will like it I'll send it tonight" "Ihave big balls"

UC: "Oh wow"

BW: "have you seen a guy naked yet"

UC: "Maddy didn't really dig ur swimsuit pics but I thought they were cool" "yes I have"

BW: "Ty I'll send some stuff for you I love to see you"

Bernard sent the UC a photo of himself wearing chaps, tight underwear, and no shirt. Bernard's genital outline is clearly visible through the underwear.

BW: "hope you like this" "Don't leave your phone laying around"

BW: "Would you like to see less cloths on"

UC: "I don't care"

Bernard sent the UC a photo of his bare erect penis and scrotum.

UC: "wow"

BW: "I have a big cock"

UC: "yeah bigger than guys my age"

BW: "I'm Glade you like it"

After Bernard asked for another picture, I sent another image of the same female associated with the undercover persona. The girl in the image is fully clothed and is making a face at the camera.

BW: "Very sexy nice boobs"

UC: "Thx"

BW: "I bet you have a boy friend s"

UC: "nope immature"

BW: "Wow a virgin" "That's a good thing"

UC: "It really sucks being 15 I want to be on my own"

BW: "I know what you mean parents are a pain in your ass some times"

UC: "Why do u like my boobs they are small"

BW: "Yes I like small may I see them"

UC: "Do other girls my age show u their boob?" "s"

BW: "Yes sometimes"

UC: "Oh ic. I got introubke last time so im not sure"

BW: "I won't tell anyone I promise" "please"

BW: "what's the hardest thing about being a woman"

UC: "I dunno never thought about that"

BW: "Mine is when I'm hardon trying to cover it up and walk because I'm big"

BW: "Do you have trouble with your period" "Some girls do"

UC: "No"

BW: "Your luck then" "sometimes it can be very painful"

BW: "what are you up to"

UC: "Nothing"

BW: "Me to just put my toy on would you like a picture"

UC: "Sure"

Bernard sent the UC two images of what looked like the shape, size, and color of a butternut squash. His underwear is down and his penis appears to be penetrating the device.

BW: "Two toys I use"

UC: "I know your only 15 I'm shure you get horny I know I did"

Bernard also sent the UC an image of his erect penis covered by a condom.

BW: "Do you like the rubber" "Hard to find xlarge" "Yes I'm fucking big"

UC: "yeah it must be difficult"

BW: "Everyone things they should be huge some girls don't like it that big it herts"

BW: "I have to be careful" "Being sore the next day after sex is common for me"

UC: "Why would u be sore"

BW: "Like if I did you .you would be a little sore because your very tight pussy"

UC: "Oh ic you probably wouldn't want me anyway"

BW: "I honey I would love to have you I would love to have sex with you"

UC: "So we can have sex"

BW: "Yes we can would you like very that"

UC: "Sure what do u want me to do"

BW: "Can I have another picture" "Anything you would like"

After Wagner requested another picture, I sent him an image of the same female undercover persona depicted in previous images sent to him. In this image, the girl was wearing a bra and panties and was lying on a bed.

BW: "for what I see I like suck on your pussy"

UC: "Never had that"

BW: "Wow you never had a blow job" "I will make cum run down your legs"

UC: "Wow"

BW: "Do you have a sex vibrator"

UC: "I don't know what that is"

Bernard then sent the UC an image of an adult sex toy attached to what appeared to be a battery pack.

BW: "You turn it on the silver part vibrates makes you cum"

BW: "Do you get horny"

UC: "Oh no I don't ever use anything like that" "I guess"

BW: "Do you ever feel that you should have sex"

UC: "I think everyone does at one point or another"

BW: "Your right so are you a virgin"

UC: "I guess" "sorry im stupid I know"

BW: "I would love to be your first" "Your not stupid at all"

BW: "We need to get together"

UC: "Would we have aex" "sex"

BW: "Yes that's why I ask about your monthly if your up to do that" "I would have to where a rubber"

UC: "Nice"

BW: "Are you ok with that"

UC: "yes sounds nice"

UC: "have u had sex with anyone as young as me. I don't want to be bad at it."

BW: "Yes ihave you will be awesome at I promise" "You just have to lay there I will show you what to do"

9. On September 21, 2020, the following communications occurred between Wagner and me acting in my undercover capacity:

UC: "Sorry I fell asleep last night" "Are we still going to have sex"

BW: "Yes I would like more pictures please" "I want to make shut it's a good idea experience for you"

UC: "What are you doing tomorrow"

BW: "I have to work what color underwear do you have on" "When do you start your pirod again"

UC: "Like second week October or so"

BW: "That's good know so are you a virgin"

UC: "Yes"

BW: "Do you play with yourself sometimes"

UC: "Sometimes not often"

BW: "There is nothing wrong with that I would love to be the first for you but it needs to be special"

UC: "Like what do you mean special"

BW: "Loosing your virigenty only happens once it should be fun you will like sex after two or three times"

UC: "So when are you thinking"

BW: "I would like more pictures of you first"

I then sent Wagner an image of the same undercover persona previously sent to Wagner.

BW: "Wow should take your top off for me I should you my stuff" "Your very sexy" "And tits" "I would love to see everything"

UC: "Im not comfortable with that" "Do I have to do that to have sex?"

BW: "Now not all you don't have to have your face in the picture .I hardly get layed" "Can I call you" "No you don't I'm ok with that" "you sent me some nice

pictures" "Just want to shut your willing" "Are you willing to get naked in front of me"

UC: "Yea"

BW: "I just want to make sure you want to get fucked"

UC: "You know it"

BW: "Then your ready for a big cock in you"

10. At this point and time, Donna Reece contacted me and advised me that Wagner continued texting M.R., the original victim, from the same number my UC had been chatting with Wagner. Reece advised he kept asking M.R. if she received his text. M.R. has not responded, and I advised Donna not to have M.R. respond.

11. The following is my continued chat with Wagner:

UC: "Maddy told me u keep texting her" "Ok later then"

BW: "Not really" "I only want to have sex with you not Maddie" "When I have sex with you I'm yours until you say I can sleep with someone else is that ok"

UC: "That sounds nice" "Just only txt me please!" "OK"

BW: "I'm in love with you" "Not Maddie"

UC: "Well she doesn't want to talk to you like I do" "So I don't want to share"

BW: "Can I ask a question"

UC: "What"

BW: "Do you have hair between your legs I your pussey"

UC: "Yes why"

BW: "some girls shave there" "you should try it"

UC: "I dunno"

BW: "When did you become a woman not a girl when you were 13 just wandering" "I have two sisters that's when they started" "there were mean after that" "I shave I love no hair on my balls"

UC: "Im sorry have to read now then to bed good nigh"

BW: "Night Sweetie"

12. On September 22, 2020, Donna Reece contacted me again and advised me that M.R. had received another message from Wagner. The message read that he wanted to thank M.R. for introducing him to her friend. I advised Donna that M.R. should not respond to the text message.

13. Spearfish Detective Collin Smith provided me with the following information regarding vehicles registered to either Bernard Wagner or his wife Connie Wagner:

LIC/9C8372. LIT/REGULAR NON-COMMERCIAL
VEHICLE. EXP/11/30/2020.
VIN/5XYPGDA37LG632132. VYR/2020. VMA/KIA.
OWN/CONNIE L WAGNER.
ADR/[REDACTED] South Dakota 57783.

LIC/MA5215. LIT/MOTORCYCLE. EXP/11/30/2020.
VIN/1HD1BJL50JY017037. VYR/1988. VMA/HD.
OWN/BERNARD A WAGNER, JR.
ADR/[REDACTED] South Dakota 57783.

LIC/9C8371. LIT/REGULAR NON-COMMERCIAL
VEHICLE. EXP/11/30/2020.
VIN/5TBBT44186S479244. VYR/2006. VMA/TOYT.
OWN/BERNARD A WAGNER JR.
ADR/[REDACTED] South Dakota 57783.

LIC/L60834. LIT/TRAILER - SMALL. EXP/11/30/2020.
VIN/5KTPS25187F193960. VYR/2007. VMA/KARA.
OWN/CONNIE J WAGNER.
ADR/[REDACTED] South Dakota 57369.

LIC/RE8609. LIT/TRAILER - SMALL. EXP/11/30/2020.
VIN/5NHUUS01XLW075393. VYR/2020. VMA/UNKN.
OWN/CONNIE J WAGNER.
ADR/[REDACTED] South Dakota 57369.

14. Detective Smith advised me that Wagner's house located at [REDACTED] [REDACTED] Spearfish, SD, 57783, has a basement apartment. Detective Smith checked several city and local records systems and does not believe a tenant currently occupies the basement apartment. Based on records, Detective Smith also does not believe tenants occupy any of the outbuildings located on the property. As such, it appears Wagner and his wife solely occupy the property.

15. Detective Smith advised Bernard works at the Chainsaw Center on Colorado Boulevard, Spearfish, SD. Detective Smith believes Bernard will be at the Chainsaw Center during the daytime hours during the week.

16. Law enforcement executed a previously obtained search warrant on Wagner's home and seized multiple devices. Wagner was at work at the time of the execution, so law enforcement went to his work to interview and arrest him on a criminal complaint. Upon contact, Wagner was in possession of two phones, the SUBJECT DEVICES, one of which he initially lied about possessing. Ultimately, he admitted to possessing both phones and using the Tracfone to communicate with two minor females. Wagner directed agents to his vehicle and permitted them to seize the SUBJECT DEVICES.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS INCLUDING
CELL PHONES

17. Based upon my training and experience, as well as information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during a search of physical premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and

specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and

make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

18. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give the target an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

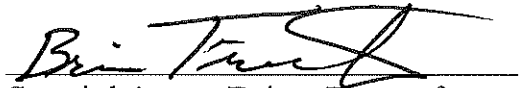
LIMIT ON SCOPE OF SEARCH

19. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

20. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, are located on the SUBJECT DEVICES, described further in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT DEVICES, authorizing the seizure and search of the items described in Attachment B.

21. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.


Special Agent Brian Freeouf
South Dakota Division of Criminal
Investigation

SUBSCRIBED and SWORN to

_____ in my presence
X by reliable electronic means

this 30th day of October, 2020.



DANETA WOLLMANN
U.S. MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Seized and Searched

The content of two cellular phones obtained during the search and arrest of Bernard Andrew Wagner, Jr. They are:

- One black Samsung Galaxy S9 in black case. IMEI: 353305092632468; and
- One black Motorola Tacfone. Model XT2005DL IMEI: 352180103523696

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely a violation of 18 U.S.C. § 2251, attempted sexual exploitation of a minor, and 18 U.S.C. § 2422(b), enticement or attempted enticement of a minor using the internet:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTERS"):
 - a. evidence of who used, owned, or controlled the COMPUTERS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTERS, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTERS of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTERS;
 - h. evidence of the times the COMPUTERS were used;

- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTERS;
 - j. documentation and manuals that may be necessary to access the COMPUTERS or to conduct forensic examinations of the COMPUTERS;
 - k. records of or information about Internet Protocol addresses used by the COMPUTERS;
 - l. records of or information about the COMPUTERS' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including
 - a. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
 - b. Records and information relating to sexual exploitation of children, including correspondence and communications between Whisper app users.
6. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
7. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones (cell phones), tablets, certain gaming devices, server computers, and network hardware.
8. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include but are not limited to internal and external hard drives, SD cards, storage disks (CDs and DVDs), flash memory, other magnetic or optical media and "cloud" storage by any provider.

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Seizure and Search of:

USA vs. 20-10-05

)
) Case No. 5:20-mj-213
)
)
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

See **ATTACHMENT A** attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 18 U.S.C. § 2251 and 18 U.S.C. § 2422(b), as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before November 13, 2020 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 10/30/20 at 9:20 am

City and state: Rapid City, SD



Judge's signature

Daneta Wollmann, U.S. Magistrate

Printed name and title

cc: AUSA Collins
kle

Return		
Case No.: 5:20-mj-213	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized: 		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: _____</p> <p style="text-align: right;">_____ Executing officer's signature</p> <p style="text-align: right;">_____ Printed name and title</p>		